IN THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Please cancel claims 1-19, 37-66, and 83-88 without prejudice.

1-19. (Canceled)

20. (Original) A computer implemented method comprising:

performing a one-way hash of an email address to generate a hashed value of the email address;

comparing the hashed value of the email address against a master do-not-email list, the master do-not-email list comprising a plurality of one-way hashed values of a set of one or more email addresses of a one or more individuals; and

determining that the individual should not be contacted if the hashed value of the email address matches one of the one-way hashed values of the set of one or more email addresses.

21. (Original) The method as in claim 20 further comprising:

collecting the email address using a data collection system.

22. (Original) The method as in claim 20 further comprising:

causing the email address to be at least one of automatically purged from a contact list, purged from a client's machine, blocked from entering a contact

email list, blocked from entering a spam list, purged from a spam list, and reported that the email address is on the master do-not-contact list.

23. (Original) A computer implemented method comprising:

collecting a set of one or more do-not-email list entries, each do-not-email list entry is a string of characters representing an email address;

applying a one-way hashing scheme to the set of one or more do-not-email list entries to convert the strings of characters into unique hashed values to create a set of one or more hashed do-not-email list entries;

transferring the set of one or more hashed do-not-email list entries to a master do-not-email list server configured to store the set of one or more hashed do-not-email list entries; and

comparing an encrypted client entry against the set of one or more hashed do-not-email list entries.

24. (Original) The method as in claim 23 wherein the encrypted client entry is a hashed value of an email address stored on a client machine, the client machine is communicable with the master do-not-email list server to check if the email information appears in the set of one or more hashed do-not-email list entries.

25. (Original) The method as in claim 24 wherein the comparing of the encrypted client entry against the set of one or more hashed do-not-email list entries allows the client machine to protect the email address.

26. (Original) The method as in claim 24 wherein the encrypted client entry is created on the client machine and wherein the email address is both stored and hashed on the client machine.

27. (Original) The method as in claim 24 wherein the comparing of the encrypted client entry against the set of one or more hashed do-not-email list entries is performed on the client machine.

28. (Original) The method as in claim 23 configuring a master do-not-email list database to be in communication with the master do-not-email list server, the master do-not-email list database configured to store the set of one or more hashed do-not-email list entries for the master do-not-email list server.

29. (Original) A computer implemented method comprising:

collecting a set of one or more do-not-email list entries, each do-not-email list entry is a string of characters representing an email address;

applying a one-way hashing scheme to the set of one or more do-not-email list entries to convert the strings of characters into unique hashed values to create a set of one or more hashed do-not-email list entries;

transferring the set of one or more hashed do-not-email list entries to a master do-not-email list server configured to store the set of one or more hashed do-not-email list entries;

requesting from the master do-not-email list server at least one hashed do-not-email list entry from the set of one or more hashed do-not email list entries to create or update a client do-not-email list on a client machine;

causing a client email entry to be hashed to create a hashed client email entry; and

comparing the hashed client email entry to the client do-not-email list to determine whether the hashed client email entry appears on the client do-not-email list.

30. (Original) The method as in claim 29 wherein the hashed client email entry is a hashed value of an email address stored on the client machine, the client machine performs the causing of the client email entry to be hashed, the client machine performs the requesting from the master do-not-email list server, and the client machine performs the comparing the hashed client email entry to the client do-not-email list.

31. (Original) The method as in claim 29 wherein the hashed client email entry is a hashed value of an email address stored on the client machine and the client machine performs the causing of the client email entry to be hashed.

32. (Original) The method as in claim 29 configuring a master do-not-email list database to be in communication with the master do-not-email list server, the master do-not-email list database configured to store the set of one or more hashed do-not-email list entries for the master do-not-email list server.

33. (Original) The method as in claim 30 wherein the comparing of the hashed client entry against the set of one or more hashed do-not-email list entries allows the client machine to protect the email address.

34. (Original) The method as in claim 29 wherein the requesting from the master do-not-email list server of at least one hashed do-not-email list entry from the set of one or more hashed do-not email list entries to create or update the client do-not-email list on the client machine is maintained by an email marketer.

35. (Original) The method as in claim 34 wherein the email marketer uses a client do-not-email list application to cause the requesting from the master do-not-email list server and to create or update the client do-not-email list on the client machine.

36. (Original) The method as in claim 35 wherein the email marketer uses the client do-not-email list application to periodically check bulk email lists maintaining by the email marketer to have email addresses associated with the set of one or more do-not-email list entries be kept free of spam.

37-65. (Canceled)

67. (Original) A computer implemented method to identify email addresses registered on a do not contact list that are in a client's list without revealing the email addresses on the do not contact list or the client's list comprising:

the client encrypting at least certain of entries on the client's list to create a plurality of encrypted entries, where each entry includes at least an email address;

the client transmitting over a network said plurality of encrypted entries from the client's list to a service for comparison to encrypted entries of the do not contact list, wherein the encrypted entries of the do not contact list were formed by encrypting information, including at least an email address, a matching of an encrypted entry from said plurality of encrypted entries from the client's list to an entry of the do-not-contact list represents that the underlying email address needs to be identified; and

the client receiving results of the comparison.

68. (Original) The computer implemented method of claim 67, wherein the client receiving results of the comparison comprises:

the client receiving back information identifying only those of said transmitted encrypted entries that matched.

69. (Original) The computer implemented method of claim 67, wherein the client receiving results of the comparison comprises:

the client receiving back information identifying only those of said transmitted encrypted entries that did not match.

70. (Original) The computer implemented method of claim 67, further comprising:

the client determining which entries on the client's list matched based on said received results; and

the client removing the matched entries from the client's list.

71. (Original) A computer implemented method to identify email addresses registered on a do-not-contact list that are in a client's list without revealing the email addresses on the do-not-contact list or the client's list comprising:

the client encrypting at least certain of entries on the client's list to create a plurality of encrypted entries, where each entry includes at least an email address;

the client transmitting over a network said plurality of encrypted entries from the client's list to a service for comparison to encrypted entries of the do-not-contact list, wherein the encrypted entries of the do-not-contact list were formed by encrypting information, including at least an email address that belongs to a minor, a matching of an encrypted entry from said plurality of encrypted entries from the client's list to an entry of the do-not-contact list represents that the underlying email address needs to be identified; and

the client receiving results of the comparison.

72. (Original) The computer implemented method of claim 71, wherein the encrypted entry belonging to the minor is automatically removed from the client's list.

73. (Original) The computer implemented method of claim 71, further comprising:

associating the email address that belongs to the minor with a parent's address.

74. (Original) The computer implemented method of claim 73, further comprising:

the client causing a notification to be sent to the parent 's address to notify the parent when there is a request to remove the contact information associating with the encrypted entry that belongs to the minor from the do-not-contact list.

75. (Original) The computer implemented method of claim 73, further comprising:

the client causing a notification to be sent to the parent 's address to notify the parent when there is an attempt to remove the contact information associating with the encrypted entry that belongs to the minor from the do-not-contact list.

76. (Original) The computer implemented method of claim 71, wherein the client receiving results of the comparison comprises:

the client receiving back information identifying only those of said transmitted encrypted entries that matched.

77. (Original) The computer implemented method of claim 71, wherein the client receiving results of the comparison comprises:

the client receiving back information identifying only those of said transmitted encrypted entries that did not match.

78. (Original) The computer implemented method of claim 71, further comprising:

the client determining which entries on the client's list matched based on said received results; and

the client removing the matched entries from the client's list.

79. (Original) A computer implemented method to identify email addresses registered on a do-not-contact list without revealing the email addresses on the do-not-contact list comprising:

a client encrypting at least certain of entries on the client's list to create a plurality of encrypted entries, where each entry includes at least an email address that does not wish to be contacted;

the client causing a comparison of said plurality of encrypted entries from the client's list to a plurality of encrypted entries of a master do-not-contact list, wherein the encrypted entries of the master do-not-contact list were formed by encrypting information, including at least an email address that belongs to a minor, a matching of an encrypted entry from said plurality of encrypted entries from the client's list to an entry of the master do-not-contact list represents that the underlying email address needs to be identified;

the client receiving results of the comparison; and

the client updating the client's list with encrypted information retrieved from the master do-not-contact list.

80. (Original) The computer implemented method of claim 79, wherein when the encrypted entry that matches one of the encrypted entries of the master do-not-contact list of belongs to the minor is automatically removed from the client's list.

81. (Original) The computer implemented method of claim 79, further comprising:

associating the email address that belongs to the minor with a parent's address.

82. (Original) The computer implemented method of claim 81, further comprising:

the client causing a notification to be sent to the parent 's address to notify the parent when there is a request to remove the contact information associating with the encrypted entry that belongs to the minor from the client's list.

83-88. (Canceled)